Cisco ACE Web Application Firewall

Product Overview

The Cisco® ACE Web Application Firewall (Figure 1) is the newest component of the Cisco Application Control Engine (ACE) family of products.

Many organizations are looking to increase efficiency and profitability through the implementation of new Web-based applications, Web 2.0 and SOA solutions. These new Web-based services provide greater flexibility and interactivity to customers, employees, and partners. At the same time, criminals have seized on exploiting these new, and often poorly secured services for such things as financial fraud, identity and data theft, denial of service attacks, and the spread of malware and remote-controlled agent software.

According to privacyrights.org, nearly a quarter of a billion records have been breached since 2005 in the US alone. In response, new and emerging regulatory requirements, like Sarbanes-Oxley, Graham-Leach-Bliley, HIPAA, PCI, Basel II, EU Data Privacy Regulation, J-SOX, and PIPEDA, in virtually every country and region in the world, place a special emphasis on protecting the access to, transmission of, and storage of sensitive information, such as the personal and financial information of customers and employees.

Of special interest is the protection of consumer financial and personal information. In response to increased identity theft incidents and security breaches, major credit card companies have collaborated to create the Payment Card Industry (PCI) Data Security Standard (DSS), which is a series of requirements to streamline and standardize how companies store and access credit card information.

The Cisco ACE Web Application Firewall helps organizations that store, process, and transmit credit card data to comply with the PCI DSS requirements. Because of its unique blend of HTML and XML security, the Cisco ACE Web Application Firewall provides a full compliance solution for the PCI DSS version 1.1's requirements in sections 6.5 and 6.6.

Section 6.6 in particular mandates that any organization handling, processing, or storing credit card information must install a Web application firewall by June 30, 2008 to protect applications against the OWASP Top 10 attacks (http://www.owasp.org/index.php/Top_10_2007.)

The Cisco ACE Web Application Firewall provides full compliance with the latest PCI requirements by combining deep Web application analysis with high-performance XML inspection and management to truly address the full range of threats associated with all new Web application services. It secures and protects Web applications from common attacks, such as identity theft, data theft, application disruption, fraud and targeted attacks. These attacks may include cross-site scripting (XSS) attacks, SQL and command injection, privilege escalation, cross-site request forgeries (CSRF), buffer overflows, cookie tampering, and Denial of Service (DoS) attacks.

The Cisco ACE Web Application Firewall's integrated Extensible Markup Language (XML) firewall capabilities extend protection for traditional HTML-based Web applications to modern XML-enabled Web services applications. The security for XML data includes XML threat mitigation such

as validating XML content to block message processing policy violations in your Web services' application traffic.

The Cisco ACE Web Application Firewall is also a full proxy security solution that provides deep message-level inspections for both request and response traffic. This enables it to not only block attacks but also to cloak your Web applications from hackers. It can also enforce privacy policies by filtering outbound traffic to prevent leakage of sensitive data such as credit cards and personal identification numbers, such as passports or social security numbers.

The Cisco ACE Web Application Firewall software license can be upgraded to include the full Cisco ACE XML Gateway software, which provides a robust set of XML performance enhancement and management tools for XML-based software applications. The Cisco ACE XML Gateway helps to ensure that all XML messages are processed without compromising security, interoperability, or reliability. It enables businesses to efficiently secure, accelerate, and integrate XML Web services with the market's most extensive policy control and end-to-end performance, which allows customers to accelerate their time-to-market and gain competitive advantage in their businesses.

Figure 1. Cisco ACE Web Application Firewall

Secure, fast, and reliable HTML and XML applications require the capability to deliver assured throughput, high concurrency, low latency, and support for critical operations such as security and availability. The Cisco ACE Web Application Firewall offers these benefits by providing:

- Bullet-proof security for your custom applications
- Extensive set of Cisco validated signatures for known malicious patterns
- Understanding of Web applications to filter and allow only legitimate traffic
- Human-assisted learning to remove the guesswork from your security configuration

The Cisco ACE Web Application Firewall offers industry-leading security processing on a high-performance network appliance to accommodate your development and deployment requirements. Whether you are showing proof of concept, securing a small set of Web-enabled applications, or deploying a broad set of Web-enabled applications enterprise wide, Cisco provides the industry-leading Web application firewall solution that scales to meet your application security, availability and performance requirements.

Features and Benefits

- Dramatically reduce exposure to expensive Web-based attacks on mission critical applications
- Deploy secure Web projects in a fraction of the time and cost of competitive solutions
- Simplify ongoing Web security management through the ability to work with SOAP and XML applications

Figure 2 shows a typical deployment, and Table 1 summarizes the features and benefits of the Cisco ACE Web Application Firewall.

Figure 2. Cisco ACE Web Application Firewall Deployment

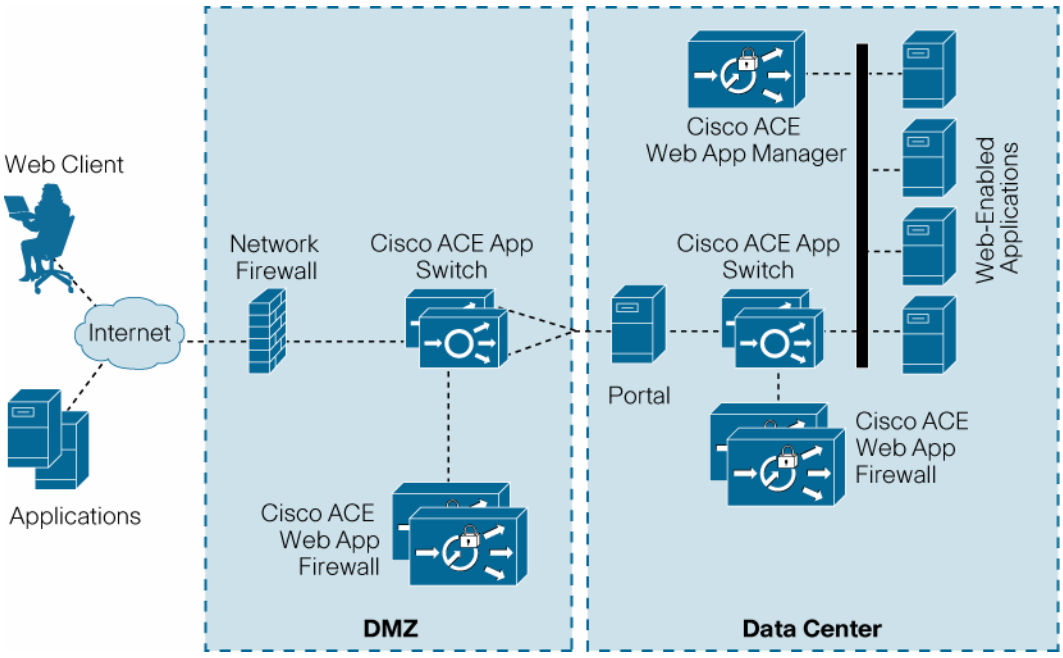

Table 1. Features and Benefits

Feature	Benefit
Web Application Security	• Support for human-assisted learning using monitor mode deployment • Defends applications against Web-based HTML and XML threats • Protects against identity theft, data theft, content and format threats, access threats, compliance, transport, and targeted attacks such as denial-of-service (DoS) attacks • Enables users to create custom rules and signatures • Offers a set of preconfigured rules that help address PCI DSS 1.1 section 6.5 and 6.6 (OWASP Top 10) requirements
Privacy	• Exerts comprehensive, enterprise wide, policy control for application access and data privacy
Encryption and Signing	• Prevents cookie tampering and maintain confidentiality of information stored in browser cookies. • Provides full FIPS-compliance, protecting against Secure Sockets Layer (SSL) key hijacking by persistently storing private SSL keys in the platform hardware
Audit and Logging	• Meets compliance requirements with audit and non repudiation capabilities
Monitoring	• Quickly debugs and monitors Web applications using sophisticated GUI • Comprehensive statistics and reporting capability
Policy-Based Provisioning and Versioning	• Increases developer productivity and improves deployment flexibility with sophisticated rollback and versioning capabilities • Quickly eliminate false positives with the ability to turn off firewall rules for specific violations with a single click. • Provides enterprise wide management accessible anywhere on the network through the Web GUI or Secure Shell (SSH) interface • Enables configuration of security policies in one centralized policy management system, without programming
Acceleration and Offloading	• Accelerates Web and XML application processing and improves server utilization by offloading computationally intensive operations such as transport security and enabling HTTP TCP session reuse. • Allows upgrades with future performance enhancements without requiring new hardware

Product Specifications

Table 2 provides software specifications, and Table 3 provides hardware specifications for the Cisco ACE Web Application Firewall.

Table 2. Product Specifications for the Cisco ACE Web Application Firewall

Item	Specification
Web Application Security	• Full reverse proxy • Monitor mode deployment • Buffer overflow • HTTP parameter manipulation, Protocol compliance • Null byte blocking • Input encoding normalization • Response filtering and rewriting • Flexible firewall actions • Cookie and session tampering • Cross-site scripting (XSS) • Command injection, SQL injection • Privacy enforcement by preventing information leak • Cryptography enforcement • Application and server error message cloaking • Referrer enforcement • Positive and negative security models • Custom rules and signatures • PCI compliance profiles
Transport Security	• Full SSL v2/3 support with configurable cipher suites • FIPS 140-2 Level 3 platforms available
Cryptographic Support	• Cryptographic algorithms including: • Advanced Encryption Standard (AES) • Data Encryption Standard (DES) • Triple DES (3DES) • Blowfish • RSA • Diffie-Helman • Digital Signature Algorithm (DSA) • Secure Hash Algorithm 1 (SHA-1) and Message-Digest 5 (MD5)
Administration	• Web user interface • Command-line interface • SSH • Simple Network Management Protocol (SNMP) • Roles-based access control (RBAC) • Delegated administration • Central policy management and distributed enforcement • Import and export of configuration, statistics, and logs
Logging, Monitoring, and Auditing	• Syslog and message and event logs • Traffic and service-level agreement (SLA) monitoring and reporting • Statistics for monitoring and various alerts and triggers • Audit trail of administrative operations

Table 3. Product Specifications: Cisco ACE Web Application Firewall Hardware

Item	Specification
Chassis	Dimensions • 1 rack unit (1RU) standard rack mount: 1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm) Weight • 37 lb (16.8 kg) fully configured (per unit, not including shipping materials)
Processor	• 2 Intel dual-core Xeon processors
Hardware Accelerators	One of the following: • 1 FIPS 140-2 Level 3–compliant 4,000 SSL TPS • 1 Non-FIPS compliant (14,000 SSL TPS)
Ports	• 4 Gigabit Ethernet ports plus a dedicated lights-out management Ethernet port
Memory	• 4 GB fixed RAM

Item	Specification
Storage	• Dual hot-swappable serial-attached Small Computer System Interface (SCSI) hard disk drive (SAS HDD) with RAID (20 GB usable)
Power	• Dual redundant; 700 watts (W)

Cisco Service and Support

Cisco takes a lifecycle approach to services and, with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Cisco services include:

- The Cisco Security Center provides one-stop shopping for early warning threat intelligence threat and vulnerability analysis, Cisco IPS signatures, and mitigation techniques. Visit and bookmark the Cisco Security Center at www.cisco.com/security.
- The Cisco Security Intellishield Alert Manager Service provides a customizable, Web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.
- Cisco Security Optimization Service: Increasingly, the network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes. This service helps integrate security into the core network infrastructure.
- Cisco SMARTnet Service delivers rapid issue resolution by giving businesses direct, anytime access to Cisco engineers, an award-winning online Support Center, machine-to-machine diagnostics on select devices and premium advance hardware replacement options.
- Cisco Software Application Support Services, plus Upgrades [SASU] ensures CSA availability, functionality, and reliability with around-the-clock access to technical support, software updates, and major upgrades

The services and support programs described in Table 4, Cisco SMARTnet® Service and Software Application Support plus Upgrades (SASU), are available as part of the Cisco ACE Web Application Firewall Service and Support solutions.

Table 4. Cisco SMARTnet and Software Application Service and Support Programs

Service and Support	Features	Benefits
Available directly from Cisco or through Cisco Certified Partners • Cisco SMARTnet Service • Cisco SASU	• 24x7 access to software updates and upgrades • 24x7 access to Cisco Technical Assistance Center (TAC) via web, phone, email • Advance replacement of hardware parts (Cisco SMARTnet Service only)	• Supplements existing staff • Helps ensure that functions meet needs • Mitigates risk • Helps enable proactive or expedited problem resolution • Lowers total cost of ownership (TCO) by using Cisco expertise and knowledge • Helps minimize network downtime

Ordering Information

Companies can choose between two versions of the Cisco ACE Web Application Firewall, depending on which cryptographic processor meets their needs. One version offers FIPS-compliant SSL acceleration rated at 4000 transactions per second (TPS); the other is rated at 10,000 TPS but is not FIPS compliant.

Table 5 provides ordering information for the Cisco ACE Web Application Firewall.

Table 5. Ordering Information

Product Options	Product Name	Part Number	Support and Services
Chassis	• Cisco ACE Web Application Firewall Appliance	• ACE-XML-K9 or • ACE-XML-NF-K9	• CON-SNT-ACEXK9 or • CON-SNT-ACEXNK9
Software	• Cisco ACE Web Application Firewall Software	• ACE-XML-SW-6.0	–
Cryptography	• FIPS-compliant SSL acceleration or • Non-FIPS-compliant SSL acceleration	• ACE-XML-FIPS or • ACE-XML-NONFIPS	• CON-SNT-ACEXFIPS or • CON-SNT-ACEXNFIP
Licensing	• Cisco ACE Web Application Firewall license or • Cisco ACE Web Application Firewall Manager license	• ACE-WAF-GAT-LICFX or • ACE-WAF-MGT-LICFX	• CON-SAU-ACEWGW or • CON-SAU-ACEWMG

For More Information

For more information about the Cisco ACE Web Application Firewall, visit http://www.cisco.com/go/waf or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-458627-01 05/08